UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/828,548	04/06/2001	Mark Linus Bauman	ROC920000258US1	4976

7590 12/15/2004

Andrew J. Dillon
BRACEWELL & PATTERSON, L.L.P
Intellectual Property Law
P.O. Box 969
Austin, TX 78767-0969

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 12/15/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/828,548	BAUMAN ET AL.	
	Examiner	Art Unit	
	Samson B Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 April 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *4*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims **1-27** have been examined.

Specification

2. The disclosure is objected because of the following informalities:

- On page 9, line 20-21, "a network adapter is utilized to connect data processing system 20 ...", has been mentioned with respect to figure 2. It should have been written as "a network adapter is utilized to connect data processing system 100 or 207".
- On page 10, line 6, "network 200 comprises a computer system ..." has been mentioned with respect to figure 2, however there is no reference on figure 2 which indicates "network 200"
- On page 7, lines 16 and on page 11, line 21 and line 24, "Figure 3A-3D ....." has been mentioned, however there is no reference on the drawing which indicates "Figure 3A-3D"
- On page 5, line 13, "United States Patent (Ser. No. 5, 241,299)" has been mentioned, It should have been "United States Patent (Ser. No. 5, 241,599)"

Drawings

3. The drawing is objected because of the following informalities:

- On page 10, line 6, "network 200 comprises a computer system ..." has been mentioned with respect to figure 2, however there is no reference on figure 2 which indicate "network 200"

- On page 7, lines 16 and on page 11, line 21 and line 24, "Figure 3A-3D ....." has been mentioned, however there is no reference on the drawing which indicates "Figure 3A-3D"

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 1-4,9-12 and 17-20** are rejected under 35 U.S.C. 103(a) as being unpatentable over Bellovin et al. (hereinafter referred to as **Bellovin**) (U.S. Patent No. 5,241.599) in view of Liao et al. (hereinafter referred as **Liao**)(U.S. Patent No. 6,263,437)

6. **As per claim 1,9 and 17 Bellovin** discloses a method for providing secure access to console functions of a computer system comprising:

- Initiating a first EKE sequence to generate a device shared secret utilizing a default associated shared secret on a system-attached device from which a console operation is desired enabled; (column 14, lines 41-44; column 5, lines 4-32)(EKE or "Encrypted key exchange" algorithm which is introduced by Bellovin and Merritt is explained on the abstract. The

invention used this algorithm and suggested also to use other similar key exchange algorithm as explained for instance on page 8 line 12. The first EKE sequence is initiated by the Alice or any computer which is communicating with the server or Bob. This is done to generate a device shared secret "R" by two parties who shares the associated default shared secret/password "P". Alice computer is the one which is interpreted by the office as the system attached device from which a console operation is desired enabled, This interpretation is given because **Bellovin** discloses on the abstract that the method is used to generate secure cryptographic "device shared secret R "over an insecure network, and both are attached devices since both Alice or Bob's computers are attached to the insecure network as shown on figure 6, ref. Num "Comm Channel")

- Generating said device shared secret from said first EKE sequence, wherein said device shared secret is utilized in place of said default device shared secret in subsequent console authentication procedures; (column 5, lines 33-45; column 5, lines 43-45) (The device shared secrete which is interpreted by the office as "R" is generated and is used in the place of the default device shared secret "P". "R" is used in place of said default device shared secret "P" in subsequent console communication as explained on column 5, lines 43-45).

Bellovin does not explicitly teach storing device shared secret within a storage location of said system and on said system-attached device. **Bellovin** does not also explicitly disclose that the initiating to a first sequence to generate a device shared secret utilizing a default device identifier so that

said the system-attached device and system will generate device shared secret.

However, in the same field of endeavor, **Liao** discloses generating and storing the identical device shared secret within a storage location of said system or server and on said system attached device or the thin client. (column 12, lines 38-40; column 14, lines 12-15)

Furthermore **Liao** discloses the thin client initiates a first encrypted key exchange request to generate a device shared secret utilizing a default device identifier so that the system- attached device and system will generate an identical device shared secret. (Column 11, lines 56-59; Figure 4, ref. Num "406")

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the storing of device shared key on both communicating devices and the utilization of the device ID to generate an identical shared key as per teachings of **Liao** in to the method of as taught by **Bellovin** for the purpose of authenticating the communicating parties and by doing so avoiding the middleman attack.

7. **Claims 25,26,27** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Liao et al**. (hereinafter referred as **Liao**)(U.S. Patent No. 6,263,437) in view of **Ramasubramani et al**. (hereinafter referred to as **Ramasubramani**) (U.S. Patent No. 6,233,577)

8. **As per claim 25 and 27**, **Liao** discloses a method of signing in authenticated users to a console function of a system, comprising:

- Determining via a first EKE/encrypted key exchange sequence whether a device identifier and associated shared secret of a system-attached device matches a stored device identifier and associated shared secret on said system; (column 11, lines 55-59; column 12, lines 22-40; column 12, lines 50-65)

Liao does not explicitly teach

- Responsive to both ends having identical shared secrets, receiving a user-entered identifier and password; responsive to said receiving,

- Initiating a second EKE sequence to determine whether said user-entered identifier and password matches a user identifier and password combination stored on a storage location of said system; and

- Granting said user access to console functions only when said second EKE sequence is successful.

However, in the same field of endeavor, **Ramasubramani** discloses

- Responsive to both ends having identical device ID, receiving a user-entered identifier and password; responsive to said receiving, (column 8, lines 41-43)

- Initiating a second EKE sequence to determine whether said user-entered identifier and password matches a user identifier and password combination stored on a storage location of said system; (Column 8, lines 57-63) and

- Granting said user access to console functions only when said second EKE sequence is successful. (Column 8, lines 63-65)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the initiating of a second EKE sequence to

determine authorization of the user as per teachings of Ramasubramani in to the determination method via a first key exchange whether or not a device identifier and the associated shared secret or SSK of both communicating devices matches as taught by **Liao** in order to provide authorization only for those users with appropriate privileges.

9. **As per claims 2, 10 and 18**, the combinations of Bellovin and Liao discloses the method as applied to claims 1, 9 and 17 above. Furthermore **Liao** discloses the method wherein said shared secret is stored in a protected manner on said system attached deivce and utilized with a device ID during each connection of said system-attached device to said system. (Column 14, lines 12-15; column 11, lines 56-59; column 12, lines 22-30)

10. **As per claims 3, 11 and 19**, the combinations of Bellovin and Liao discloses the method as applied to claims 2, 10 and 18 above. Furthermore **Liao** discloses the method further comprising encrypting operator authentication data flowing between said system-attached device and said system utilizing said shared secret. (Abstract, lines 16-19)

11. **As per claims 4, 12 and 20** the combinations of Bellovin and Liao discloses the method as applied to claims 2, 10 and 18 above. Furthermore **Liao** discloses the method further comprising encrypting operator authentication data flowing between said system-attached device and said system utilizing a hash of said shared secret. (Abstract, lines 16-19, Column 12, lines 50-67; column 11, lines 26-28) (The client private value is suggested to be generated by a one-way hash functions, by the same analogy encrypting operator authentication data flowing between said system-attached device and said system could be encrypted by a hash of said shared secret)

12. **Claims 5-7,13-15 and 21-23** are rejected under 35 U.S.C. 103(a) as being unpatentable over Bellovin et al (hereinafter referred to as Bellovin) (U.S. Patent No. 5,241.599) in view of Liao et al (hereinafter referred as Liao) (U.S. Patent No. 6,263,437) further in view of **Ramasubramani et al**. (hereinafter referred to as **Ramasubramani**) (U.S. Patent No. 6,233,577)

13. **As per claims 5-7,13-15, and 21-23**, the combinations of Bellovin and Liao discloses the method as applied to claims 2, 10 and 18. Furthermore **Liao** discloses the method of determining via a first EKE/encrypted key exchange sequence whether a device identifier and associated shared secret of a system-attached device matches a stored device identifier and associated shared secret on said system; (column 11, lines 55-59; column 12, lines 22-40; column 12, lines 50-65)

The combinations of Bellovin and Liao does not explicitly teach responsive to an establishment of a first console session that authenticates said system-attached device, instantiating a second EKE sequence to authenticate a console operator utilizing a default user identifier and password; and storing said user identifier and password in a protected area of said storage location of said system.

However, in the same field of endeavor, **Ramasubramani** discloses

- Responsive to both ends having identical device ID, receiving a user-entered identifier and password; responsive to said receiving, (column 8, lines 41-43)

- Initiating a second EKE sequence to determine whether said user-entered identifier and password matches a user identifier and password combination stored on a storage location of said system; (Column 8, lines 57-63)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the initiating of a second EKE sequence to determine authorization of the user as per teachings of **Ramasubramani** in to the determination method via a first key exchange whether or not a device identifier and the associated shared secret or SSK of both communicating devices matches as taught by the combinations of **Bellovin** and **Liao** in order to provide authorization only for those users with appropriate privileges.

14. **Claims 8,16 and 24** are rejected under 35 U.S.C. 103(a) as being unpatentable over Bellovin et al (hereinafter referred to as Bellovin) (U.S. Patent No. 5,241.599) in view of Liao et al (hereinafter referred as Liao) (U.S. Patent No. 6,263,437) further in view of **Ramasubramani et al**. (hereinafter referred to as **Ramasubramani**) (U.S. Patent No. 6,233,577) further in view of I/O Concepts Inc, Title Console Consolidation System Overview.(hereinafter referred to as **I/O Concepts**) (reference U)

15. **As per claims 8,16 and 24**, the combinations of Bellovin, Liao and Ramasubramani discloses the method as applied to claims 5, 13 and 21.Furthermore Furthermore **Liao** discloses the method of determining via a first EKE/encrypted key exchange sequence whether a device identifier and associated shared secret of a system-attached device matches a stored device identifier and associated shared secret on said system; (column 11, lines 55-59; column 12, lines 22-40; column 12, lines 50-65)

The combinations of Bellovin and Liao does not explicitly teach responsive to an establishment of a first console session that authenticates said system-attached device, instantiating a second EKE sequence to authenticate a console operator utilizing a default user identifier and password; and storing said user identifier and password in a protected area of said storage location of said system.

However, in the same field of endeavor, **Ramasubramani** discloses

- Responsive to both ends having identical device ID, receiving a user-entered identifier and password; responsive to said receiving, (column 8, lines 41-43)

- Initiating a second EKE sequence to determine whether said user-entered identifier and password matches a user identifier and password combination stored on a storage location of said system; (Column 8, lines 57-63)

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the initiating of a second EKE sequence to determine authorization of the user as per teachings of Ramasubramani in to the determination method via a first key exchange whether or not a device identifier and the associated shared secret or SSK of both communicating devices matches as taught by the combinations of Bellovin and **Liao** in order to provide authorization only for those users with appropriate privileges.

The combinations of **Bellovin**, **Liao** and **Ramasubramani** does not explicitly teach enabling multiple console sessions for different systems on a single console device.

However, in the same field of endeavor, **I/O Concepts** discloses that console consolidation allows multiple operators to access and work in console sessions simultaneously and **I/O Concepts** further discloses console consolidation

software allows console sessions to be moved form workstation to workstation with ease, and even allows mainframe consoles to be displayed on more than one workstation at any one time.(Page 1, 2nd paragraph and see also page 4, Under the Title "Console Consolidation At a Glance", line 2).

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to provide the facility of enabling multiple console sessions for different systems on a single console device as per teachings of **I/O Concepts**, in to the method as taught by the combinations of **Bellovin, Liao** and **Ramasubramani**, in order to provide affordable and flexible console consolidation.

16. **As per claim 26**, the combinations of Liao and Ramasubramani discloses the method as applied to claims 25 above. Furthermore **Ramasubramani** discloses the method further comprising encrypting data transmitted during said second EKE sequence utilizing a shared secret generated during said first EKE sequence.(Column 14, lines 37-41)

Conclusion

17. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.(See PTO-Form 892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799.

The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA
S.L
12/06/2004

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100